

Security of continuous-variable quantum key distribution against general attacks

Anthony Leverrier¹, Raúl García-Patrón², Renato Renner¹, Nicolas J. Cerf³

¹*Institute for Theoretical Physics, ETH Zurich, 8093 Zurich, Switzerland*

²*Max-Planck Institut für Quantenoptik, Hans-Kopfermann Str. 1, D-85748 Garching, Germany and*

³*Quantum Information and Communication, Ecole Polytechnique de Bruxelles,
CP 165, Université Libre de Bruxelles, 1050 Bruxelles, Belgium*

(Dated: August 27, 2012)

We prove the security of Gaussian continuous-variable quantum key distribution against arbitrary attacks in the finite-size regime. The novelty of our proof is to consider symmetries of quantum key distribution in phase space in order to show that, to good approximation, the Hilbert space of interest can be considered to be finite-dimensional, thereby allowing for the use of the postselection technique introduced by Christandl, Koenig and Renner (*Phys. Rev. Lett.* 102, 020504 (2009)). Our result greatly improves on previous work based on the de Finetti theorem which could not provide security for realistic, finite-size, implementations.

Quantum key distribution (QKD), the art of generating a secret key among distant parties in an untrusted environment, is certainly the most studied quantum cryptographic primitive. Since the seminal papers of Bennett and Brassard [1] and Ekert [2], considerable progress has been made in terms of security analysis [3]. Security against arbitrary attacks has been proven for several protocols, even in the realistic finite-size regime. This is quite remarkable because of the very large number of possible attacks against which security needs to be guaranteed. Security proofs generally circumvent this problem by using the natural permutation invariance of most QKD protocols which allows to restrict the analysis to the much smaller class of *collective* attacks, where the eavesdropper interacts independently and identically with every communication signal. In an entanglement-based description of QKD, this amounts to assume that the joint state $\rho_{A^n B^n}$ that the two legitimate parties, Alice and Bob, hold after the initial distribution of entanglement, has an identical and independently distributed (i.i.d.) structure $\rho_{A^n B^n} = \sigma_{AB}^{\otimes n}$, where n is the number of quantum signals exchanged during the protocol.

One usually achieves this reduction from general to collective (i.i.d.) attacks thanks to either de Finetti-type theorems [4] or the postselection technique [5]. Unfortunately, these tools cannot be directly applied to continuous-variable (CV) protocols because they require the dimension of the Hilbert space to be finite (and small compared to n). However, by prepending a suitable energy test to the protocol, it is still possible to use a specific variant of the de Finetti theorem and derive the security of CV protocols, but only for impractically large values of n [6]. Here, we wish to improve the analysis of [6] to prove the security of continuous-variable QKD in the realistic finite-size scenario.

The specificity of CV protocols is that the detection consists of (homodyne or heterodyne) measurements of the light-field quadratures (see Ref. [7] for a review). From an experimental point of view, they present many advantages over discrete-variable protocols. Most importantly, they can be implemented with standard telecom components and are compatible with Wavelength Divi-

sion Multiplexing [8], which is an important advantage when integrating QKD into real-world telecommunication networks. Moreover, quadrature measurements do not require any photon counters and higher repetition rates can be achieved. Distribution of secret keys over long distances (more than 80 km) is currently achievable [9], making CV protocols competitive with respect to their discrete-variable counterparts. Their security analysis, however, is technically challenging due to the infinite-dimensional nature of the relevant Hilbert space.

Among CV protocols, the so-called Gaussian ones are the most popular ones, primarily due to their experimental simplicity. In a prepare-and-measure scheme, one party, Alice, prepares coherent or squeezed states with a Gaussian modulation and sends them to a receiver, Bob, who applies a homodyne or heterodyne measurement. In the equivalent entanglement-based scheme, Alice prepares an entangled two-mode squeezed vacuum state (the continuous-variable equivalent of the Bell pair), keeping one mode and sending the other one to Bob through the quantum channel. Then both parties measure their respective mode with either a homodyne or heterodyne detection, obtaining two strings of correlated real-valued data. Finally, Alice and Bob extract a secret key through information reconciliation and privacy amplification.

The security of Gaussian protocols in the asymptotic regime is rather well understood: de Finetti's theorem guarantees that collective attacks are optimal [6] and Gaussian attacks are known to be optimal among collective ones [10, 11]. On the other hand, their security in the much more relevant finite-size regime is less clear, due to the difficulty of the reduction from general attacks to the i.i.d. scenario. Currently, two results in this direction are known for CV protocols, either based on a de Finetti theorem as stated above or on an uncertainty relation. The de Finetti approach [6] is unsuitable in practical scenarios because n , the required number of signals exchanged during the protocol, is too large. The second approach, using an entropic uncertainty inequality [12], works for more reasonable values of n but unfortunately does not converge towards the asymptotic key rate secure against collective attacks in the limit of infinitely many

signals. Consequently, the tolerated losses are quite low, corresponding to a few hundred meters only.

In the remainder of this Letter, we first explain how to modify a protocol secure against collective attacks by the addition of an initial test in order to enforce a certain property of the entangled state, namely a low single-mode photon number. Then, we apply these ideas to the specific case of a Gaussian protocol where Bob performs heterodyne measurements and establish its security against arbitrary attacks.

Main result.— In this paper, we give the first security proof of CV QKD against general attacks, which guarantees a secret key rate for realistic experimental regimes, in terms of losses and noise. As in [6, 12], this is achieved by prepending an initial test to a protocol already proven secure against collective attacks. The purpose of the test is to verify that the quantum state shared by Alice and Bob is well-approximated by a state living in a reasonably small dimensional Hilbert space. Then, one can use the postselection technique [5] which shows roughly that if a (permutation-invariant) protocol is ϵ -secure against collective attacks, then it is $\tilde{\epsilon}$ -secure against general attacks with $\tilde{\epsilon} = \epsilon \times \text{poly}(n)$.

Our result improves that of Ref. [6] for two reasons. First the postselection technique guarantees much better bounds than the approach based on a de Finetti theorem when reducing general to collective attacks [13]. Moreover, and this is in fact the main technical contribution of the present work, we exploit specific symmetries of the CV QKD protocol in phase space instead of the usual and less powerful permutation symmetry. We therefore obtain a very tight bound on the effective dimension of the quantum state. More precisely, the QKD protocol is invariant if Alice and Bob process their respective modes with global conjugate passive linear transformations of their n modes before performing their measurements. This “rotational-symmetry” in phase space is better suited to analyze CV protocols [20], allowing to precisely bound the effective number of photons per mode from the results of random quadrature measurements. This is in stark contrast with Ref. [6] where the test only exploited the permutation symmetry of the protocol.

QKD protocols and their security.— A QKD protocol is a CP map from the infinite-dimensional Hilbert space $(\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes n}$, corresponding to the initially distributed entanglement, to the set of pairs (S_A, S_B) of l -bit strings (Alice and Bob’s final keys, respectively) and C , a transcript of the classical communication. In order to assess the security of a given QKD protocol \mathcal{E} in a composable framework, one compares it with an ideal protocol [14]. Such an ideal protocol \mathcal{F} can be constructed (at least in principle) by concatenating the protocol with a map \mathcal{S} taking (S_A, S_B, C) as input and outputting the triplet (S, S, C) where the string S is a perfect secret key (uniformly distributed and unknown to Eve) with the same length as S_A , that is $\mathcal{F} = \mathcal{S} \circ \mathcal{E}$. Then, a protocol will be called ϵ -secure if the advantage in distinguishing

it from an ideal version is not larger than ϵ . This advantage is quantified by (one half of) the diamond norm defined by

$$\|\mathcal{E} - \mathcal{F}\|_\diamond := \sup_{\rho_{ABE}} \|(\mathcal{E} - \mathcal{F}) \otimes \text{id}_{\mathcal{K}}(\rho_{ABE})\|_1, \quad (1)$$

where the supremum is taken over $(\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes(n+k)} \otimes \mathcal{K}$ for any auxiliary system \mathcal{K} .

Prepending a test.— Our main technical result is a reduction of the security against general attacks to that against collective attacks, for which security has already been proved in earlier work. Let us therefore suppose that our CV QKD protocol of interest, \mathcal{E}_0 , is secure against collective attacks. We will slightly modify it by prepending an initial test \mathcal{T} . More precisely, \mathcal{T} is a CP map taking a state in a slightly larger Hilbert space, $(\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes(n+k)}$, measuring k randomly chosen modes (identical for Alice and Bob) and comparing the measurement outcome to a value fixed in advance. The test succeeds if this norm is small, meaning that the global state is compatible with a state containing only a low number of photons per mode, that is a state well-described in a low dimensional Hilbert space, which leads to better bounds when using the post-selection technique. Depending on the outcome, either the whole protocol aborts, or one applies \mathcal{E}_0 on the n remaining modes. A more precise description is provided as part of the “heterodyne protocol” below.

For our purpose, it is crucial that the test is feasible in practice. This is the case here since it only involves k additional homodyne (or heterodyne) measurements compared to the original scheme \mathcal{E}_0 , with k much smaller than n , as well as applying some classical post processing to Alice and Bob’s data.

In order to establish that the protocol $\mathcal{E} := \mathcal{E}_0 \circ \mathcal{T}$ is ϵ -secure against arbitrary attacks, one needs to bound $\|\mathcal{E} - \mathcal{F}\|_\diamond$. The postselection theorem [5] allows one to bound the diamond norm between such maps by simply considering i.i.d. states (i.e. the equivalent of collective attacks), but only when the maps act on finite dimensional spaces. We address this issue by introducing another CP map \mathcal{P} which projects a state in $(\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes n}$ onto a low-dimensional Hilbert space $(\overline{\mathcal{H}}_A \otimes \overline{\mathcal{H}}_B)^{\otimes n}$ where $\overline{\mathcal{H}}_A := \text{Span}(|0\rangle, |1\rangle, \dots, |d_A - 1\rangle)$ and $\overline{\mathcal{H}}_B := \text{Span}(|0\rangle, |1\rangle, \dots, |d_B - 1\rangle)$ are respectively a d_A and a d_B -dimensional subspace of the Fock spaces \mathcal{H}_A and \mathcal{H}_B . We define (virtual) protocols $\tilde{\mathcal{E}} := \mathcal{E}_0 \circ \mathcal{P} \circ \mathcal{T}$ and $\tilde{\mathcal{F}} := \mathcal{S} \circ \tilde{\mathcal{E}}$. The security of the protocol \mathcal{E} is then a consequence of the following derivation:

$$\begin{aligned} \|\mathcal{E} - \mathcal{F}\|_\diamond &\leq \|\tilde{\mathcal{E}} - \tilde{\mathcal{F}}\|_\diamond + \|\mathcal{E} - \tilde{\mathcal{E}}\|_\diamond + \|\mathcal{F} - \tilde{\mathcal{F}}\|_\diamond \\ &\leq \|\tilde{\mathcal{E}} - \tilde{\mathcal{F}}\|_\diamond + \|\mathcal{E}_0 \circ (\text{id} - \mathcal{P}) \circ \mathcal{T}\|_\diamond \\ &\quad + \|\mathcal{F}_0 \circ (\text{id} - \mathcal{P}) \circ \mathcal{T}\|_\diamond \\ &\leq \|\tilde{\mathcal{E}} - \tilde{\mathcal{F}}\|_\diamond + 2\|(\text{id} - \mathcal{P}) \circ \mathcal{T}\|_\diamond, \end{aligned} \quad (2)$$

where we used the triangle inequality and the fact that the CP maps \mathcal{E}_0 and \mathcal{F}_0 cannot increase the diamond

norm. The first term can be bounded thanks to the postselection theorem because $\tilde{\mathcal{E}}$ and $\tilde{\mathcal{F}}$ are finite dimensional, and it can be made arbitrary small at the price of reducing slightly the key rate. The second term can be bounded thanks to the following theorem for which we give a proof sketch for the “heterodyne protocol” below (and a full proof in Appendix A).

Theorem 1. (Informal.) *For any rotationally-invariant state $\rho_{ABE} \in (\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes(n+k)} \otimes \mathcal{K}$,*

$$\|(\text{id}_{\mathcal{H}^{\otimes n}} - \mathcal{P}) \circ \mathcal{T} \otimes \text{id}_{\mathcal{K}}(\rho_{ABE})\|_1 \leq \epsilon, \quad (3)$$

where ϵ is a function of k, n , the dimensions d_A and d_B for the projection \mathcal{P} and the value of the threshold in the test \mathcal{T} .

Description for the protocol with heterodyne detection.— Let us now consider a specific example of a QKD protocol \mathcal{E}_0 . For the sake of clarity, we choose (arguably) the simplest one [15]. In the prepare-and-measure version of the protocol, Alice prepares n coherent states which are modulated with a Gaussian distribution, and sent through the quantum channel. In the equivalent entangled version of the protocol, for which we prove security, Alice prepares n two-mode squeezed vacuum states, measures one mode of each state with a heterodyne detection and sends the other one through the quantum channel. Bob then performs a heterodyne measurement of the states he receives. This means that he measures both quadratures q and p for each mode. This is achieved by sending the modes on a balanced beam-splitter and measuring the q quadrature for one output mode and the p quadrature for the other one. At the end of this process, Alice and Bob have access to two correlated vectors in \mathbb{R}^{2n} , \vec{x}_A for Alice and \vec{x}_B for Bob. Then, they perform the reconciliation procedure [16] in order to extract a common string, and finally privacy amplification [17] to distill their final secret keys, S_A and S_B , respectively.

This protocol is invariant under the action of conjugate passive symplectic operations (beam splitters and phase shifts) because these correspond to some orthogonal transformation $R \in O(2n)$ of the quadratures in phase space. Specifically, if such an operation is applied, then Alice and Bob’s vectors become $R\vec{x}_A$ and $R^T\vec{x}_B$ (see Appendix E for details), meaning that the effect of the beam splitters and phase shifts can be undone by simply applying the inverse rotation on the classical data.

We assume in the following that the protocol \mathcal{E}_0 is secure against collective attacks, in the sense that for any pure state $\rho_{ABE} \in \mathcal{H}_A \otimes \mathcal{H}_B \otimes \mathcal{H}_E$ where $\mathcal{H}_E \cong \mathcal{H}_A \otimes \mathcal{H}_B$, the quantity $\|(\mathcal{E}_0 - \mathcal{F}_0) \otimes \text{id}_{\mathcal{K}}(\rho_{ABE})\|_1$ can be made exponentially small in n , say $2^{-c\delta^2 n}$, at the price of reducing the secret key rate by an arbitrary small fraction δ compared to the asymptotic optimal rate, for some constant $c > 0$. We note that despite being proven secure against collective attacks in the asymptotic limit [10, 11, 18], the security of \mathcal{E}_0 for finite size attacks is not yet completely

understood in the sense that the precise values of c and δ are not currently known: this is due to the difficulty of estimating a covariance matrix in the finite-size regime (see [19]).

As we mentioned above, we will prove the security of a slightly modified protocol, noted \mathcal{E} which starts with $n + k$ modes (instead of n in the case of \mathcal{E}_0), k of which being used to conduct a test \mathcal{T} . If the test passes, corresponding roughly to a scenario where the state does not contain too many photons, then Alice and Bob proceed with the protocol \mathcal{E}_0 , otherwise they abort. The test \mathcal{T} is in fact only applied to Bob’s classical data. Indeed, we assume here that Alice prepares her state in a trusted environment meaning that her reduced state is an $(n+k)$ -modal thermal state. Note that one could easily remove this assumption and also apply \mathcal{T} to Alice’s state.

The test consists in first choosing a random rotation R in $\mathbb{R}^{2(n+k)}$ (with the appropriate measure) and applying it to the $2(n+k)$ -dimensional vector corresponding to Bob’s measurement outcomes (as well as to Alice’s vector). Let us denote by $q_1, p_1, q_2, p_2, \dots, q_k, p_k$ the first $2k$ coordinates of Bob’s rotated vector and define the variable $Y_k := \sum_{i=1}^k (q_i^2 + p_i^2)$. The coordinates correspond to heterodyne measurements of k modes of ρ_B^{n+k} after being processed through an appropriate network of beam splitters and phase shifts (see Appendix E). The test \mathcal{T} is characterized by 2 parameters: a positive number Y_{test} and k . The test passes if $Y_k \leq Y_{\text{test}}$ and fails otherwise. More precisely, because the test commutes with the measurement, it can equivalently be seen as a map from $(\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes(n+k)}$ to $(\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes n}$ (plus an additional bit encoding whether the test passed or not) that returns the n remaining modes when it passes and an “abort” state when it fails.

It is also useful to describe the CP map \mathcal{P} characterized by three numbers, n , and the local dimensions d_A and d_B . It corresponds to the binary outcome measurement in $(\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes n}$ described by the POVM $\{P_A^{\otimes n} \otimes P_B^{\otimes n}, \mathbb{1} - P_A^{\otimes n} \otimes P_B^{\otimes n}\}$ where P_A and P_B are the single-mode projectors on \mathcal{H}_A and \mathcal{H}_B , respectively, defined as $P_{A/B} = |0\rangle\langle 0| + |1\rangle\langle 1| + \dots + |d_{A/B}-1\rangle\langle d_{A/B}-1|$.

In order to establish Theorem 1, we will bound the probability p_{bad} of the following bad event: “the state passes the test and the projection onto $P_A^{\otimes n} \otimes P_B^{\otimes n}$ fails” for some initial state $\rho_{AB}^n \in (\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes n}$. Let us note $\tilde{\rho}_{AB}^n$ the unnormalized state after the test when it passed; the probability of passing the test is simply $p_{\text{test}} = \text{tr} \tilde{\rho}_{AB}^n$ and $p_{\text{bad}} = \text{tr} [(1 - \mathcal{P}) \circ \mathcal{T}(\rho_{AB}^{n+k})]$. One can bound p_{bad} in the following way:

$$\begin{aligned} p_{\text{bad}} &= \text{tr} (\text{id}_{AB} - P_A^{\otimes n} \otimes P_B^{\otimes n}) \tilde{\rho}_{AB}^n \\ &\leq \text{tr} [(\text{id}_A - P_A^{\otimes n}) \tilde{\rho}_A^n] + \text{tr} [(\text{id}_B - P_B^{\otimes n}) \tilde{\rho}_B^n] \\ &\leq \text{tr} [(\text{id}_A - P_A^{\otimes n}) \rho_A^n] + \text{tr} [(\text{id}_B - P_B^{\otimes n}) \tilde{\rho}_B^n] \end{aligned} \quad (4)$$

where we used the union bound and the fact that Alice does apply the test. The first term is easy to compute because the state of Alice, a multimode thermal state, is well known: $\rho_A^n = \rho_{\text{thermal}}^{\otimes n}$ with $\rho_{\text{thermal}} =$

$\sum_{k=0}^{\infty} \frac{\lambda^k}{(1+\lambda)^{k+1}} |k\rangle\langle k|$ for a state with λ photons per mode. The value of λ is a parameter of the protocol and should be optimized given the expected characteristics of the quantum channel. The union bound gives

$$1 - \text{tr}(P_A^{\otimes n} \rho_A^n) \leq n(1 - \text{tr}(P_A \rho_{\text{thermal}})) = n \left(\frac{\lambda}{1+\lambda} \right)^{d_A}.$$

In particular, choosing $d_A = \frac{\log(n/\epsilon_A)}{\log(1+1/\lambda)}$ for the dimension of Alice's Hilbert space leads to $1 - \text{tr}(P_A^{\otimes n} \rho_A^n) \leq \epsilon_A$.

Bounding the second term in Eq. (4) is much trickier because one cannot assume that Bob's state ρ_B^n is Gaussian or that it even has an i.i.d. structure. This is because it corresponds to the output of the unknown quantum channel controlled by Eve. Here, we will make use of the specific symmetries of the QKD protocol in phase space in order to simplify greatly the problem. In general, most protocols are invariant under permutations of the subsystems of Alice and Bob. This means that the state ρ_{AB}^n (and therefore also ρ_B^n) can be assumed to display this invariance. However, CVQKD protocols such as the one considered here respect a much stronger symmetry: they are invariant when Alice and Bob apply to their respective $(n+k)$ modes conjugate passive linear transformations, implemented by any network of beamsplitters and phase shifts [18, 20] (see Appendix E for details). Here, it is crucial that the test \mathcal{T} respects the symmetry, and this can be enforced *at the level of classical data* by the choice of the random subspace T of $\mathbb{R}^{2(n+k)}$ (as explained before).

Thanks to this symmetry, one can assume that the state ρ_B^{n+k} of Bob (before applying the test \mathcal{T}) is rotationally invariant, that is, left invariant under the action of any network of passive linear operations on their $n+k$ modes. Such states were already studied in Ref. [21] where a de Finetti theorem was established: if sufficiently many modes of ρ_B^{n+k} are traced out, then the remaining state is close to a mixture of thermal states. Intuitively, one then expects that the second term of Eq. 4 behaves like the first one, and this is what we prove rigorously. Before we explain how to bound $\text{tr}(P_B^{\otimes n} \tilde{\rho}_B^n)$, we recall two useful properties of states, such as ρ_B^{n+k} , which are rotationally invariant [21]. First, these states are mixtures of generalized $(n+k)$ -mode Fock states $\sigma_p^{n+k} := 1/(\binom{n+k+p-1}{p}) \sum_{p_1+\dots+p_m=p} |p_1, p_2, \dots, p_m\rangle\langle p_1, p_2, \dots, p_m|$, where $|p_1, \dots, p_m\rangle$ is the product of Fock states with p_1 photons in the first mode, p_2 photons in the second mode, etc, and the sum is taken over all states with a total number of p photons in $n+k$ modes. This means that there exist $\lambda_0 \geq 0, \lambda_1 \geq 0, \dots$ such that $\rho_B^{n+k} = \sum_{p=0}^{\infty} \lambda_p \sigma_p^{n+k}$. The second useful property is that the Wigner function $W(q_1, p_1, \dots, q_{n+k}, p_{n+k})$ of ρ_B^{n+k} is isotropic, that is only depending on the norm of the vector $(q_1, p_1, \dots, q_{n+k}, p_{n+k})$. The same also holds for the Q-function of the state, that is the prob-

ability distribution of the outcomes of the heterodyne measurements.

Let us introduce another random variable $Z_n := 1/(2n) \sum_{i=1}^n q_{k+i}^2 + p_{k+i}^2$, corresponding to the norm of Bob's heterodyne measurements for the n modes of ρ_B^{n+k} not measured during the test \mathcal{T} . We show in the appendix that the probability ϵ_{test} of passing the test but Z_n being much larger than Y_{test} is exponentially small in k when the value of Y_{test} is chosen slightly larger the expected variance of Bob's measurement results (see Lemma A.2). In turn, this implies that the *total* number of photons in the state ρ_B^n is bounded by $O(nY_{\text{test}})$ (see Lemma A.3). Finally, we show that the projection over the space $\overline{\mathcal{H}}_B^{\otimes n}$ succeeds with high probability if $d_B = \dim \overline{\mathcal{H}}_B = O(\log \frac{2n}{\epsilon})$ (see Lemma A.4). This finally provides a bound on $\|(1 - \mathcal{P}) \circ \mathcal{T}\|_{\diamond}$ and proves Theorem 1.

We now put things together and establish that protocol \mathcal{E} is secure against general attacks. First, choosing d_A and d_B on the order of $O(\log(n/\epsilon_{\text{test}}))$, one obtains $\|(1 - \mathcal{P}) \circ \mathcal{T}\|_{\diamond} \leq \epsilon_{\text{test}}$. Second, assuming that the original protocol \mathcal{E}_0 is secure against collective attacks, the diamond norm $\|\tilde{\mathcal{E}} - \tilde{\mathcal{F}}\|_{\diamond}$ can be bounded by $2^{-c\delta^2 n + O(\log^2(n/\epsilon_{\text{test}}))}$ using the postselection technique where the dimension of the relevant Hilbert space $\overline{\mathcal{H}}_A \otimes \overline{\mathcal{H}}_B$ is $d_A d_B = O(\log^2(n/\epsilon_{\text{test}}))$ (see [5] for details). This shows that protocol \mathcal{E} is ϵ -secure against general attacks with

$$\epsilon = 2^{-c\delta^2 n + O(\log^2(n/\epsilon_{\text{test}}))} + 2\epsilon_{\text{test}}. \quad (5)$$

Conclusion.—We have proved that Gaussian continuous-variable QKD protocols, using a Gaussian distribution of coherent states and homodyne or heterodyne measurements, are secure against arbitrary attacks. Our proof exploits the specific symmetries in phase-space of Gaussian QKD protocols and uses a simple test to ensure that the global state shared between Alice and Bob is well described by assigning a low dimensional Hilbert space to each mode. This allows one to use the postselection technique introduced in Ref. [5] for discrete-variable protocols. Our result greatly improves on a previous one using a de Finetti theorem which could not be applied to prove the security of protocols in realistic experimental implementations. Finally, our analysis indicates that in order to prove the security of any QKD protocol, one should exploit all the available symmetries of the protocol, beyond the traditional permutation.

Acknowledgements.— This work was supported by the SNF through the National Centre of Competence in Research “Quantum Science and Technology” (grant No. 200020- 135048), the European Research Council (grant No. 258932), the Humboldt foundation and the F.R.S.-FNRS under project HIPERCOM.

-
- [1] C. Bennett and G. Brassard, in *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing* (1984), vol. 175.
 - [2] A. Ekert, Phys. Rev. Lett. **67**, 661 (1991).
 - [3] V. Scarani, H. Bechmann-Pasquinucci, N. Cerf, M. Dušek, N. Lütkenhaus, and M. Peev, Rev. Mod. Phys. **81**, 1301 (2009).
 - [4] R. Renner, Nat. Phys. **3**, 645 (2007).
 - [5] M. Christandl, R. König, and R. Renner, Phys. Rev. Lett. **102**, 020504 (2009).
 - [6] R. Renner and J. I. Cirac, Phys. Rev. Lett. **102**, 110504 (2009).
 - [7] C. Weedbrook, S. Pirandola, R. García-Patrón, N. J. Cerf, T. C. Ralph, J. H. Shapiro, and S. Lloyd, Rev. Mod. Phys. **84**, 621 (2012).
 - [8] B. Qi, W. Zhu, L. Qian, and H. Lo, New J. Phys. **12**, 103042 (2010).
 - [9] P. Jouguet, S. Kunz-Jacques, A. Leverrier, P. Grangier, and E. Diamanti, submitted to QCRYPT 2012 (2012).
 - [10] R. García-Patrón and N. J. Cerf, Phys. Rev. Lett. **97**, 190503 (2006).
 - [11] M. Navascués, F. Grosshans, and A. Acín, Phys. Rev. Lett. **97**, 190502 (2006).
 - [12] F. Furrer, T. Franz, M. Berta, A. Leverrier, V. Scholz, M. Tomamichel, and R. Werner, Arxiv preprint arXiv:1112.2179 (2011).
 - [13] L. Sheridan, T. Le, and V. Scarani, New J. Phys. **12**, 123019 (2010).
 - [14] J. Müller-Quade and R. Renner, New J. Phys. **11**, 085006 (2009).
 - [15] C. Weedbrook, A. M. Lance, W. P. Bowen, T. Symul, T. C. Ralph, and P. K. Lam, Phys. Rev. Lett. **93**, 170504 (2004).
 - [16] P. Jouguet, S. Kunz-Jacques, and A. Leverrier, Phys. Rev. A **84**, 062317 (2011).
 - [17] R. Renner, Ph.D. thesis, ETH Zurich (2005), <http://arxiv.org/abs/quant-ph/0512258>.
 - [18] A. Leverrier and P. Grangier, Phys. Rev. A **81**, 062314 (2010).
 - [19] A. Leverrier, F. Grosshans, and P. Grangier, Phys. Rev. A **81**, 062343 (2010).
 - [20] A. Leverrier, E. Karpov, P. Grangier, and N. J. Cerf, New J. Phys. **11**, 115009 (2009).
 - [21] A. Leverrier and N. J. Cerf, Phys. Rev. A **80**, 010102 (2009).
 - [22] A. Leverrier, Phys. Rev. A **85**, 022339 (2012).
 - [23] B. Laurent and P. Massart, The Annals of Statistics **28**, 1302 (2000).
 - [24] Arvind, B. Dutta, N. Mukunda, and R. Simon, Pramana **45**, 471 (1995).
-

Appendix

In this appendix, we detail the various technical results used in the main text. In Appendix A, we explicitly state our main theorem for the continuous-variable protocol where Bob uses heterodyne detection. The proof of the main theorem uses three lemmas which are established in Appendices B, C and D. In Appendix E, we detail why the protocol is invariant under the action of a network of beamsplitters and phase shifts, justifying the symmetry assumption made on Bob's quantum state.

The rest of the appendix is devoted to protocols where Bob performs a homodyne detection instead of a heterodyne one. We state our main theorem in that case in Appendix F. We prove in Appendix G that Bob's state can again be considered invariant under the action of beamsplitters and phase shifts. Our main theorem uses two of the same lemmas as in the heterodyne case and a variant of the third one which is established in Appendix H.

Appendix A: Main theorem for the heterodyne protocol

In order to make use of the relevant symmetries in phase space, the test itself should be invariant under the application of an arbitrary network of beamsplitters and phase-shifts on Bob's $(n+k)$ modes before he proceeds with his measurement. This can be enforced by actively symmetrizing the state, which can be done at the level of classical data (see Ref. [22] for a discussion on this active symmetrization).

Bob randomly chooses a random unitary U from the Haar measure on the unitary group $U(n+k)$. Then, he symmetrizes his state thanks to the network of beamsplitters and phase shifts applying the transformation U on the annihilation (b_1, \dots, b_{n+k}) and creation operators $(b_1^\dagger, \dots, b_{n+k}^\dagger)$ of his $(n+k)$ modes through

$$b_i \rightarrow \sum_{j=1}^{n+k} U_{i,j} b_j \quad \text{and} \quad b_i^\dagger \rightarrow \sum_{j=1}^{n+k} U_{i,j}^* b_j^\dagger \quad (\text{A1})$$

and finally measures his $(n+k)$ modes with a heterodyne detection. The state $\rho^{\otimes(k+n)}$ held by Bob after this symmetrization is called rotationally invariant.

Crucially, Bob can also first measure his state with a heterodyne detection and only then implement U by applying the symplectic transformation S given by

$$S := \begin{pmatrix} \text{Re}(U) & -\text{Im}(U) \\ \text{Im}(U) & \text{Re}(U) \end{pmatrix} \quad (\text{A2})$$

to his classical vector of measurements. This is true because the symmetrization in phase-space commutes with the heterodyne measurement (see Appendix E for details).

We denote $(q_1, p_1, \dots, q_{n+k}, p_{n+k})$ the classical vector Bob obtains after this procedure. Thanks to the symmetrization, without loss of generality, the test \mathcal{T} can be applied to the first k modes, that is to the data $(q_1, p_1, \dots, q_k, p_k)$.

We now state our main theorem for the protocol with heterodyne detection.

Theorem A.1 (Heterodyne protocol). *Let $\epsilon, Y_{\text{test}} > 0$ be fixed parameters. Let $Y_k = \frac{1}{k} \sum_{i=1}^k (q_i^2 + p_i^2)$ be the average of Bob's (squared) heterodyne measurement outcomes on the first k modes of his state after symmetrization, and let ρ^n be the state of the n remaining modes. Let $d_B := \frac{\log(4n/\epsilon)}{\log(1+1/d_0)}$ where $d_0 := g(\frac{\epsilon}{4}) Y_{\text{test}}$ (and g is defined in Eq. A9) and let $\overline{\mathcal{H}}_B = \text{Span}\{|0\rangle, \dots, |d_B - 1\rangle\}$ be the finite dimensional Hilbert space spanned by states with less than d_B photons. Then the probability that $Y_k \leq Y_{\text{test}}$ and that the projection of ρ^n onto $\overline{\mathcal{H}}_B^{\otimes n}$ fails is less than ϵ .*

In order to prove Theorem A.1, we need to introduce some operators acting on some subspace of $\mathcal{H}_B^{\otimes(n+k)}$. To keep notation simple, we use the subscript k (resp. n) when the operator acts on $\mathcal{H}_B^{\otimes k}$ (resp. $\mathcal{H}_B^{\otimes n}$) corresponding to the first k modes (resp. the last n modes) of the symmetrized state. Let us define the POVM elements T_k, T_n, U_n and V_n on $\mathcal{H}^{\otimes n}$ as follows:

- \mathcal{T}_k acting on $\mathcal{H}^{\otimes k}$ corresponding to a failed test, meaning that the value of the observable Y_k is larger than T_{test} :

$$\mathcal{T}_k := \frac{1}{\pi^k} \int_{\sum_{i=1}^k |\alpha_i|^2 \geq Y_{\text{test}}} |\alpha_1\rangle\langle\alpha_1| \cdots |\alpha_k\rangle\langle\alpha_k| d\alpha_1 \cdots d\alpha_k, \quad (\text{A3})$$

- T_n is the projector onto products of coherent states $|\alpha_1\rangle \cdots |\alpha_n\rangle \in \mathcal{H}_B^{\otimes n}$ such that $\sum_{i=1}^n |\alpha_i|^2 \geq nd_0$:

$$T_n := \frac{1}{\pi^n} \int_{\sum_{i=1}^n |\alpha_i|^2 \geq nd_0} |\alpha_1\rangle\langle\alpha_1| \cdots |\alpha_n\rangle\langle\alpha_n| d\alpha_1 \cdots d\alpha_n, \quad (\text{A4})$$

- U_n is the projector onto the subspace of $\mathcal{H}^{\otimes n}$ spanned by states with more than nd_0 photons

$$U_n := \sum_{m=nd_0+1}^{\infty} \Pi_m^n, \quad (\text{A5})$$

where we introduced the projector Π_m^n on the subspace spanned by n -mode states containing m photons:

$$\Pi_m^n = \sum_{m_1 + \cdots + m_n = m} |m_1 \cdots m_n\rangle\langle m_1 \cdots m_n|. \quad (\text{A6})$$

- V_n is the projector onto the subspace of $\mathcal{H}^{\otimes n}$ such that at least one mode contains at least d_B photons:

$$V_n := \mathbb{1} - P_B^{\otimes n}, \quad (\text{A7})$$

where $P_B := |0\rangle\langle 0| + \cdots + |d_B - 1\rangle\langle d_B - 1|$.

With these notations, Theorem A.1 simply gives an upper bound on $p_{\text{bad}} := \text{tr}[V_n(1 - \mathcal{T}_k)\rho^{n+k}]$ for any rotationally invariant state $\rho^{n+k} \in \mathcal{H}_B^{\otimes(n+k)}$. The quantity p_{bad} is the probability that the state passes the test and that the projection on the finite-dimensional subspace $\overline{\mathcal{H}}_B^{\otimes n}$ fails.

The proof of the theorem uses the following variants of three technical lemmas proven in Sections B, C and D of this appendix. We first state Lemma A.2 which is a corollary of a result proven in Section B.

Lemma A.2. *Let $\mathbf{X} = (X_1, \dots, X_{k+n})$ be a vector of \mathbb{C}^{n+k} . Let U be a random unitary transformation of $U(n+k)$ drawn from the Haar measure, and define $\mathbf{Y} = U\mathbf{X}$. Then*

$$\Pr \left[\frac{1}{n} \sum_{i=1}^n |Y_{k+i}|^2 \geq g(\delta) \frac{1}{k} \sum_{i=1}^k |Y_i|^2 \right] \leq \delta \quad (\text{A8})$$

where

$$g(\delta) = \frac{1 + 2\sqrt{\frac{\log(1/\delta)}{2n}} + \frac{2\log(2/\delta)}{2n}}{1 - \sqrt{\frac{2}{k}} \log\left(\frac{2}{\delta}\right)}. \quad (\text{A9})$$

By construction, the vector $Y = (Y_1, \dots, Y_{n+k})$ is uniformly distributed on the complex sphere in \mathbb{C}^{n+k} with radius $\|Y\|$, and consequently, the real vector $(\text{Re}(Y_1), \text{Im}(Y_1), \dots, \text{Re}(Y_{n+k}), \text{Im}(Y_{n+k}))$ is uniformly distributed on the corresponding real sphere in $\mathbb{R}^{2(n+k)}$. Lemma A.2 is then a special case of Lemma B.1.

The following lemma is proved in Section C.

Lemma A.3.

$$U_n \leq 2T_n. \quad (\text{A10})$$

Our final lemma quantifies the maximum number of photons in a single mode for a rotationally invariant state with nd photons in n modes, except with a small probability:

Lemma A.4. *Let m_1, \dots, m_n be the random variables corresponding to photon counting measurements of the n modes of the state σ_{nd}^n which is a uniform mixture of states with nd photons in n modes. Then, the following bound holds:*

$$\Pr \left[\max_{i=1 \dots n} m_i \geq \frac{\log\left(\frac{2n}{\epsilon}\right)}{\log(1 + 1/d)} \right] \leq \epsilon. \quad (\text{A11})$$

Proof of Theorem A.1. We fix $d_0 := g\left(\frac{\epsilon}{4}\right) Y_{\text{test}}$ and $d_B := \frac{\log(4n/\epsilon)}{\log(1+1/d_0)}$. From Lemma A.2, we know that

$$\text{tr } T_n(\mathbb{1}_k - T_k)\rho^{n+k} \leq \frac{\epsilon}{4} \quad (\text{A12})$$

for any rotationally invariant state ρ^{n+k} . From Lemma A.3, we obtain

$$\text{tr } U_n(\mathbb{1}_k - T_k)\rho^{n+k} \leq \frac{\epsilon}{2} \quad (\text{A13})$$

and Lemma A.4 shows that

$$\text{tr } (1 - U_n)V_n\rho^{n+k} \leq \frac{\epsilon}{2} \quad (\text{A14})$$

for any rotationally invariant state ρ^{n+k} .

Using that $V_n \leq V_n(1 - U_n) + U_n$, one finally has:

$$p_{\text{bad, Bob}} := \text{tr } [(V_n \circ \mathcal{T})\rho^{n+k}] \quad (\text{A15})$$

$$= \text{tr } [V_n(\mathbb{1}_k - T_k)\rho^{n+k}] \quad (\text{A16})$$

$$\leq \text{tr } [(1 - U_n)V_n(\mathbb{1}_k - T_k)\rho^{n+k}] + [U_n(\mathbb{1}_k - T_k)\rho^{n+k}] \quad (\text{A17})$$

$$\leq \text{tr } [(1 - U_n)V_n\rho^{n+k}] + 2\text{tr } T_n(\mathbb{1}_k - T_k)\rho^{n+k} \quad (\text{A18})$$

$$\leq \frac{\epsilon}{2} + 2 \times \frac{\epsilon}{4} \quad (\text{A19})$$

$$\leq \epsilon. \quad (\text{A20})$$

□

Appendix B: Concentration of measure on the sphere

In this section, we establish the following result which implies Lemma A.2.

Lemma B.1. *If the vector $\mathbf{X} = (X_1, \dots, X_{k+n})$ is uniformly distributed on the unit sphere of \mathbb{R}^{n+k} , then*

$$\Pr \left[\frac{1}{n} \sum_{i=1}^n X_{k+i}^2 \geq g(\delta) \frac{1}{k} \sum_{i=1}^k X_k^2 \right] \leq \delta \quad (\text{B1})$$

where

$$g(\delta) = \frac{1 + 2\sqrt{\frac{\log(2/\delta)}{n}} + \frac{2\log(2/\delta)}{n}}{1 - 2\sqrt{\frac{1}{k} \log\left(\frac{2}{\delta}\right)}}. \quad (\text{B2})$$

We do not prove Lemma B.1 directly because manipulating normalized vectors on the sphere is not very convenient. We use instead the natural invariance of the problem and first show that it is sufficient to prove the lemma for independent normal variables instead of vectors on the unit sphere. This is the case because a uniformly chosen vector on the sphere can be obtained by drawing n independent normal variables and normalizing the corresponding vector.

Let X_1, \dots, X_n be such independent normal random variables: $X_i \sim \mathcal{N}(0, 1)$, and let us define the following quantities:

$$Y_k = \frac{1}{k} \sum_{i=1}^k X_i^2 \quad \text{and} \quad Z_n = \frac{1}{n} \sum_{i=1}^n X_{k+i}^2. \quad (\text{B3})$$

Note that the normalized random vector $\tilde{\mathbf{X}} = \frac{1}{\sqrt{\sum_{i=1}^{n+k} X_i^2}} (X_1, \dots, X_{n+k})$ is uniformly distributed on the unit sphere of \mathbb{R}^{n+k} . In particular, it is sufficient to prove that

$$\Pr [Z_n \geq g(\delta)Y_k] \leq \delta \quad (\text{B4})$$

in order to establish the lemma.

Let us proceed with the proof of Eq. B4. We first notice that for any $A > 0$,

$$\Pr[Z_n \geq g(\delta)Y_k] \leq \Pr[Y_k \leq A] + \Pr[Z_n \geq g(\delta)A]. \quad (\text{B5})$$

We can now bound this two probabilities using the fact that Y_k and Z_n are independent random variables, with a $\chi^2(k)$ and a $\chi^2(n)$ distribution, respectively. To this end, we use two bounds on χ^2 distributions established by Laurent and Massart [23]:

$$\Pr\left[Y_k \leq 1 - 2\sqrt{\frac{x}{k}}\right] \leq \exp(-x) \quad \text{and} \quad \Pr\left[Z_n \geq 1 + 2\sqrt{\frac{x}{n}} + \frac{2x}{n}\right] \leq \exp(-x). \quad (\text{B6})$$

Choosing $x = \log(2/\delta)$ in both cases gives:

$$\Pr\left[Y_k \leq 1 - 2\sqrt{\frac{\log(2/\delta)}{k}}\right] \leq \frac{\delta}{2} \quad \text{and} \quad \Pr\left[Z_n \geq 1 + 2\sqrt{\frac{\log(2/\delta)}{n}} + \frac{2\log(2/\delta)}{n}\right] \leq \frac{\delta}{2}. \quad (\text{B7})$$

Taking $A := 1 - 2\sqrt{\frac{1}{k} \log\left(\frac{2}{\epsilon}\right)}$ concludes the proof of Lemma B.1.

Appendix C: Proof of Lemma A.3

In this section, we prove Lemma A.3 which we recall here.

Lemma A.3. *Let T_n and U_n be defined as*

$$T_n := \frac{1}{\pi^n} \int_{\sum_{i=1}^n |\alpha_i|^2 \geq nd_0} |\alpha_1\rangle\langle\alpha_1| \cdots |\alpha_n\rangle\langle\alpha_n| d\alpha_1 \cdots d\alpha_n, \quad (\text{C1})$$

and

$$U_n := \sum_{m=nd_0+1}^{\infty} \Pi_m^n \quad \text{with} \quad \Pi_m^n = \sum_{m_1+\cdots+m_n=m} |m_1 \cdots m_n\rangle\langle m_1 \cdots m_n|. \quad (\text{C2})$$

Then, the following inequality holds:

$$U_n \leq 2T_n. \quad (\text{C3})$$

1. Some preliminaries

The following integrals will be useful. For $a > 0$, let us define:

$$I_n(a) = \int_{y_i \geq 0, \sum_{i=1}^n y_i \geq a} e^{-y_1 - y_2 - \cdots - y_n} dy_1 \cdots dy_n \quad (\text{C4})$$

and

$$J_n(k, a) = \int_{y_i \geq 0, \sum_{i=1}^n y_i \geq a} \frac{y_1^k}{k!} e^{-y_1 - y_2 - \cdots - y_n} dy_1 \cdots dy_n. \quad (\text{C5})$$

These integrals can be computed explicitly.

Lemma C.1.

$$I_n(a) = e^{-a} \sum_{k=0}^{n-1} \frac{a^k}{k!} \quad (\text{C6})$$

$$J_n(k, a) = \frac{\Gamma(k+1, a)}{\Gamma(k+1, 0)} + e^{-a} \sum_{m=k+1}^{k+n} \frac{a^m}{m!}. \quad (\text{C7})$$

Proof. The first equality is proved by induction. It is clear that $I_1(a) = e^{-a}$. Then:

$$1 - I_{n+1}(a) = \int_{y_i \geq 0, \sum_{i=1}^{n+1} y_i \leq a} e^{-y_1 - y_2 \cdots - y_{n+1}} dy_1 \cdots dy_{n+1} \quad (C8)$$

$$= \int_0^a dy_{n+1} e^{-y_{n+1}} \int_{y_i \geq 0, \sum_{i=1}^n y_i \leq a - y_{n+1}} e^{-y_1 - y_2 \cdots - y_n} dy_1 \cdots dy_n \quad (C9)$$

$$= \int_0^a dy_{n+1} e^{-y_{n+1}} (1 - I_n(a - y_{n+1})) \quad (C10)$$

$$= \int_0^a dy_{n+1} e^{-y_{n+1}} \left(1 - e^{-a + y_{n+1}} \sum_{k=0}^{n-1} \frac{(a - y_{n+1})^k}{k!} \right) \quad (C11)$$

$$= 1 - e^{-a} - e^{-a} \int_0^a \sum_{k=0}^{n-1} \frac{(a - y)^k}{k!} dy \quad (C12)$$

$$= 1 - e^{-a} - e^{-a} \sum_{k=0}^{n-1} \frac{a^{k+1}}{(k+1)!} \quad (C13)$$

$$= 1 - e^{-a} \sum_{k=0}^n \frac{a^k}{k!} \quad (C14)$$

$$(C15)$$

$$J_n(k, a) = 1 - \int_{y_i \geq 0, \sum_{i=1}^n y_i \leq a} \frac{y_1^k}{k!} e^{-y_1 - y_2 \cdots - y_n} dy_1 \cdots dy_n \quad (C16)$$

$$= 1 - \int_0^a dy_1 \frac{y_1^k}{k!} e^{-y_1} \int_{y_i \geq 0, \sum_{i=2}^n y_i \leq a - y_1} e^{-y_2 - y_3 \cdots - y_n} dy_2 \cdots dy_n \quad (C17)$$

$$= 1 - \int_0^a dy_1 \frac{y_1^k}{k!} e^{-y_1} (1 - I_{n-1}(a - y_1)) \quad (C18)$$

$$= 1 - \int_0^a dy_1 \frac{y_1^k}{k!} e^{-y_1} \left(1 - e^{-a + y_1} \sum_{m=0}^{n-1} \frac{(a - y_1)^m}{m!} \right) \quad (C19)$$

$$= \frac{\Gamma(k+1, a)}{\Gamma(k+1, 0)} + e^{-a} \sum_{m=0}^{n-1} \int_0^a \frac{y^k (a - y)^m}{k! m!} dy \quad (C20)$$

where $\Gamma(s, x) = \int_x^\infty t^{s-1} e^{-t} dt$ is the incomplete gamma function Using the fact that

$$\int_0^a x^k (a - x)^m dx = \frac{k! m! a^{k+m+1}}{(k+m+1)!}, \quad (C21)$$

one obtains

$$J_n(k, a) = \frac{\Gamma(k+1, a)}{\Gamma(k+1, 0)} + e^{-a} \sum_{m=0}^{n-1} \frac{(a)^{k+m+1}}{(k+m+1)!} \quad (C22)$$

$$= \frac{\Gamma(k+1, a)}{\Gamma(k+1, 0)} + e^{-a} \sum_{m=k+1}^{k+n} \frac{a^m}{m!} \quad (C23)$$

$$(C24)$$

□

2. Proof of Lemma A.3

Integrating over the n phases gives:

$$T_n = \sum_{k_1, \dots, k_n} \int_{x_i \geq 0, \sum_{i=1}^n x_i \geq nd_0} \prod_{i=1}^n e^{-x_i} \frac{x_i^{k_i}}{k_i!} dx_i |k_1 \dots k_n\rangle \langle k_1 \dots k_n|. \quad (\text{C25})$$

Because of its rotation invariance in phase-space, the operator T_n can be written as a mixture of Π_k^n . Let us note $q_k \geq 0$ the corresponding coefficients: $T_n = \sum_{k=0}^{\infty} q_k \Pi_k^n$. Considering the term $\langle k, 0, \dots, 0 | T_n | k, 0, \dots, 0 \rangle$, it is easy to see that $q_k = J_n(k, nd_0)$.

The proof is then immediate by noticing that the sequence $\frac{\Gamma(k+1, a)}{\Gamma(k+1, 0)} = q_k - e^{-a} \sum_{m=k+1}^{k+n} \frac{a^m}{m!}$ (where we used the result of Lemma C.1) is positive and increasing with k for all $a \geq 0$. Here, $\Gamma(s, x) := \int_x^{\infty} t^{s-1} e^{-t} dt$ refers to the incomplete Gamma function. This means that for $k \geq nd_0 + 1$,

$$q_k \geq \frac{\Gamma(nd_0 + 1, nd_0)}{\Gamma(nd_0 + 1, 0)} + e^{-a} \sum_{m=k+1}^{k+n} \frac{a^m}{m!} \geq \frac{\Gamma(nd_0 + 1, nd_0)}{\Gamma(nd_0 + 1, 0)} \geq \frac{1}{2}, \quad (\text{C26})$$

where we used that $\frac{\Gamma(x+1, x)}{\Gamma(x+1, 0)}$ is lower bounded by $1/2$ for all $x \geq 0$. This allows us to conclude that

$$U_n \leq 2T_n. \quad (\text{C27})$$

Appendix D: Proof of Lemma A.4

The set of vectors $\mathbf{X} = (X_1, \dots, X_n)$ such that $\sum_{i=1}^n X_i = k$ and $X_1 \geq m$ contains $a_{k-m}^n := \binom{n+k-m-1}{k-m}$ elements. Let us note $p_k(m, n)$ the probability that the maximum of X_i is greater than m if one measures the photon number for the state σ_k^n :

$$p_k(m, n) = \Pr \left[\max_{i=1 \dots n} X_i \geq m \text{ s.t. } \sum_{i=1}^n X_i = k \right]. \quad (\text{D1})$$

The union bound gives:

$$p_k(m, n) \leq \Pr \left[X_1 \geq m \text{ s.t. } \sum_{i=1}^n X_i = k \right] + \dots + \Pr \left[X_n \geq m \text{ s.t. } \sum_{i=1}^n X_i = k \right] \quad (\text{D2})$$

$$\leq n \frac{a_{k-m}^n}{a_k^n} = n \frac{(n+k-m-1)!k!}{(n+k-1)!(k-m)!} = \frac{n(n+k)}{n+k-m} \frac{(n+k-m)!k!}{(n+k)!(k-m)!}. \quad (\text{D3})$$

Let $x > 0$, then Stirling approximation formula reads (here \log is the natural logarithm):

$$nx \log n + nx(\log x - 1) + \frac{1}{2} \log n + \frac{1}{2} \log x + \log \sqrt{2\pi} \leq \log(nx)! \leq nx \log n + nx(\log x - 1) + \frac{1}{2} \log n + \frac{1}{2} \log x + 1. \quad (\text{D4})$$

Let us introduce the variables d and δ such that $k = dn$ and $m = \delta n$. Then

$$\log \frac{(n+k-m)!k!}{(n+k)!(k-m)!} = \log(n(d+1-\delta))! + \log(nd)! - \log(n(d+1))! - \log(n(d-\delta))! \quad (\text{D5})$$

$$\leq -n \{g(d) - g(d-\delta)\} + \frac{1}{2} \log \frac{d(d+1-\delta)}{(d+1)(d-\delta)} + 2 - \log 2\pi \quad (\text{D6})$$

where

$$g(x) = (x+1) \log(x+1) - x \log x. \quad (\text{D7})$$

This gives

$$\log p_k(m, n) \leq -n \{g(d) - g(d-\delta)\} + \log n + \frac{1}{2} \log \frac{d(d+1)}{(d-\delta)(d-\delta+1)} + 2 - \log 2\pi \quad (\text{D8})$$

The function g is concave which implies that $g(d) - g(d - \delta) \geq \delta g'(d) = \delta \log(1 + 1/d)$, and therefore

$$-\log p_k(m, n) \geq n\delta \log(1 + 1/d) - \log n + \frac{1}{2} \log \frac{(d+1)(d+1-\delta)}{d(d-\delta)} - 2 + \log 2\pi \quad (\text{D9})$$

$$\geq n\delta \log(1 + 1/d) - \log n - 2 + \log 2\pi \quad (\text{D10})$$

$$\geq n\delta \log(1 + 1/d) - \log n - \log 2 \quad (\text{D11})$$

$$(\text{D12})$$

Choosing $m = \frac{\log(2n/\epsilon)}{\log(1+1/d)}$ gives $p_k(m, n) \leq \epsilon$ and proves Lemma A.4.

Appendix E: Symmetry of the state for heterodyne detection

In this section, we show that the symplectic transformation applied in phase-space commutes with the heterodyne detection. The compact subgroup of the symplectic group $\text{Sp}(2N, \mathbb{R})$ consisting of phase shifts and beamsplitters is usually noted $K(n)$ in the literature and is isomorphic to the unitary group $U(N)$ (see for instance Ref. [24]). We note $\vec{a} := (\hat{a}_1, \dots, \hat{a}_N)$ and $\vec{a}^\dagger := (\hat{a}_1^\dagger, \dots, \hat{a}_N^\dagger)$ the vectors of annihilation and creation operators of the N modes considered. Then, in the Heisenberg picture, under a symplectic transformation, the \hat{a} 's and \hat{a}^\dagger 's transform independently as:

$$\vec{a} \rightarrow U\vec{a}, \quad \text{and} \quad \vec{a}^\dagger \rightarrow U^*\vec{a}^\dagger, \quad (\text{E1})$$

where U is a unitary matrix.

Moreover, defining $V = \text{Re}(U)$ and $W = -\text{Im}(U)$ the real and imaginary parts of U such that $U = V - iW$, the displacement vector $(\vec{x}, \vec{p})^T := (x_1, \dots, x_N, p_1, \dots, p_N)^T$ is transformed as

$$\begin{pmatrix} \vec{x} \\ \vec{p} \end{pmatrix} \rightarrow \begin{pmatrix} V & W \\ -W & V \end{pmatrix} \begin{pmatrix} \vec{x} \\ \vec{p} \end{pmatrix}. \quad (\text{E2})$$

In the quantum key distribution protocol, both Alice and Bob perform a heterodyne measurement of their respective $n + k$ modes. The probability distribution of their outcomes is given by the Q -function of the state $\rho_{AB}^{n+k} \in (\mathcal{H}_A \otimes \mathcal{H}_B)^{\otimes(n+k)}$: $Q_\rho(\vec{x}_A, \vec{p}_A, \vec{x}_B, \vec{p}_B)$. From the description given above of the subgroup $K(n)$, it appears that the Q -function associated with the "rotated" state $\rho' := (\mathcal{U}_A \otimes \mathcal{U}_B^*)\rho_{AB}^{n+k}(\mathcal{U}_A \otimes \mathcal{U}_B^*)^\dagger$ (where \mathcal{U} is the representation of the symplectic transformation corresponding to the unitary U) is simply:

$$Q_{\rho'}(\vec{x}'_A, \vec{p}'_A, \vec{x}'_B, \vec{p}'_B) = Q_\rho(V\vec{x}_A - W\vec{p}_A, W\vec{x}_A + V\vec{p}_A, V\vec{x}_B + W\vec{p}_B, -W\vec{x}_B + V\vec{p}_B). \quad (\text{E3})$$

This local (and classical) transformation of the coordinates can be applied by Alice and Bob. In other words, the quantum transformation corresponding to the networks of beamsplitters and phase-shifts commutes with the heterodyne measurement.

Moreover, if one makes sure that the test (i.e., the choice of the random $2k$ -dimensional subspace of $\mathbb{R}^{2(n+k)}$) respects the symmetry above, then the post processing of the QKD protocol commutes with the map $\mathcal{U}_A \otimes \mathcal{U}_B^*$, meaning that the state ρ_{AB}^{n+k} can be considered invariant under such maps. In particular, the state held by Bob, $\rho_B^{n+k} := \text{tr}_A \rho_{AB}^{n+k}$ is invariant under any \mathcal{U} consisting in beamsplitters and phase shifts.

Appendix F: Main theorem for the homodyne protocol

We now consider a protocol where Alice sends coherent states with a Gaussian modulation and Bob performs homodyne detection with a random quadrature chosen uniformly in $[0, 2\pi]$ for each of his $n + k$ modes.

In the following, we note X_1, \dots, X_{n+k} the random variables corresponding to the $n + k$ quadrature measurement outcomes for Bob. We assume that for each mode, Bob chooses a random direction $\theta \in [0, \pi/2]$ in phase space. Then, he chooses to measure the quadrature either along θ (which we call a q measurement) or along $\theta + \pi/2$ (this is the p measurement). We will show in Section G that Bob's state can be assumed to be rotationally invariant.

Our main result is summarized by the following theorem.

Theorem F.1. *Let $\epsilon, Y_{\text{test}} > 0$ be fixed parameters. Let $Y_k = \frac{1}{k} \sum_{i=1}^k X_i^2$ be the average of Bob's (squared) homodyne measurement outcomes on the first k modes of his symmetrized state, and let ρ^n be the state of his n remaining modes. Let $d_0 := 2g(\frac{\epsilon}{16})Y_k$. We choose n large enough so that $e^{-\beta n} \leq \frac{\epsilon}{16}$ with $\beta := c_0 d_0 - \frac{\log d_0}{2}$ and $c_0 := (1 - 1/\sqrt{2})^2$. Let $d_B = \frac{\log(4n/\epsilon)}{\log(1+1/d_0)}$. Let $\overline{\mathcal{H}}_B = \text{Span}\{|0\rangle, \dots, |d_B - 1\rangle\}$ be the finite dimensional Hilbert space spanned by states with less than d_B photons. Then the probability that $Y_k \leq Y_{\text{test}}$ and that the projection of ρ^n onto $\overline{\mathcal{H}}_B^{\otimes n}$ fails is less than ϵ .*

The main novelty compared to the heterodyne protocol is the introduction of the operator W_n , corresponding to the projection on the event $[Z_n \geq d_0/2]$, where $Z_n = \frac{1}{n} \sum_{i=1}^k X_{k+i}^2$. Let us define the random variable $s_i \in \{q_i, p_i\}$ corresponding to a quadrature measurement for the mode i , either q or p . Then, we can define a string $\mathbf{s} \in \{q, p\}^n$ as being the n quadrature measurement outcomes when measuring the state ρ^n . With these notations,

$$W_n = \frac{1}{2^n} \sum_{\mathbf{s} \in \{q, p\}^n} P^{Z_n(\mathbf{s}) \geq d_0/2}. \quad (\text{F1})$$

We prove the following result in Section H.

Lemma F.2.

$$T_n \leq 2W_n + e^{-\beta n} \mathbb{1}_n \quad (\text{F2})$$

where $\beta = c_0 d_0 - \frac{\log d_0}{2}$ and $c_0 = (1 - 1/\sqrt{2})^2$.

The proof of Theorem F.1 then follows exactly the same lines as that of Theorem A.1.

Appendix G: Symmetry of Bob's state for the protocol with homodyne detection

Let $\rho^{n+k} = \sum_{\vec{i}, \vec{j}} a_{\vec{i}, \vec{j}} |i_1, i_2, \dots, i_{n+k}\rangle \langle j_1, j_2, \dots, j_{n+k}|$ be Bob's $n + k$ -mode state.

The measurement protocol is the following:

- for each mode j , Bob draws θ_j uniformly in $[0, 2\pi]$ and measures the quadrature along $\cos \theta_j q_j + \sin \theta_j p_j$. He obtains a measurement outcome x_j . It is actually sufficient to pick θ from the set $\{0, 2\pi \frac{1}{d_B}, 2\pi \frac{2}{d_B}, \dots, 2\pi \frac{d_B-1}{d_B}\}$.
- Bob then randomly chooses an orthogonal transformation R in \mathbb{R}^{n+k} and applies it to his vector $\vec{x} = (x_1, \dots, x_{n+k})$.
- finally, Bob informs Alice of his choices of θ_j and R .

Crucially, the transformation R can be equivalently obtained by applying a network of beam splitters on the $n + k$ modes.

Because of the random choice of the measured quadratures, the state ρ^{n+k} can be considered invariant under the application of $U(\theta_j) = e^{i\theta_j a_j^\dagger a_j}$. This means that

$$\rho^{n+k} \propto \int_{\vec{\theta} \in [0, 2\pi]^n} \left(\prod_{j=1}^n U(\theta_j) \right) \rho \left(\prod_{j=1}^n U(-\theta_j) \right) d\vec{\theta} \quad (\text{G1})$$

$$\propto \sum_{\vec{i}, \vec{j}} a_{\vec{i}, \vec{j}} |i_1, i_2, \dots, i_{n+k}\rangle \langle j_1, j_2, \dots, j_{n+k}| \int_{\vec{\theta} \in [0, 2\pi]^{n+k}} e^{i\theta_1(i_1-j_1)} \dots e^{i\theta_{n+k}(i_{n+k}-j_{n+k})} d\vec{\theta} \quad (\text{G2})$$

$$\propto \sum_{\vec{i}} a_{\vec{i}, \vec{i}} |i_1, i_2, \dots, i_{n+k}\rangle \langle i_1, i_2, \dots, i_{n+k}|. \quad (\text{G3})$$

Because of the random rotation of the measurement results, the state can also be considered invariant under the action of any network of beamsplitters. In particular, it should be invariant when swapping any two modes and when applying infinitesimal beamsplitters. The first condition shows that the coefficient $a_{\vec{i}} := a_{\vec{i}, \vec{i}}$ is invariant when permuting the coordinates of the vector \vec{i} . The invariance under infinitesimal beamsplitters guarantees that $a_{i_1, i_2, i_3, \dots, i_{n+k}} = a_{i_1+1, i_2-1, i_3, \dots, i_{n+k}} = a_{i_1+\dots+i_{n+k}, 0, \dots, 0}$. In particular, the coefficient $a_{\vec{i}}$ only depends on the total number of photons i in the n modes.

Finally, the state ρ^{n+k} can be assumed to be a mixture of the states σ_i^{n+k} defined as:

$$\sigma_i^{n+k} = \frac{1}{\binom{n+k+i-1}{i}} \sum_{\sum i_j = i} |i_1, \dots, i_{n+k}\rangle \langle i_1, \dots, i_{n+k}|. \quad (\text{G4})$$

Appendix H: Proof of Lemma F.2

1. Preliminaries

Let us define $F(\vec{a})$ as

$$F(\vec{a}) = \frac{1}{\pi^{n/2}} \int_{\|\vec{z}\|^2 \geq nd_0} d\vec{z} e^{-\|\vec{z}-\vec{a}\|^2}. \quad (\text{H1})$$

The spherical symmetry of the function guarantees that $F(\vec{a})$ only depends on the norm of \vec{a} . Let us note $a = \|\vec{a}\|$. In the following, it is sometimes useful to think of the vector \vec{a} as $\vec{a} = (a, 0, \dots, 0)$. The following bound will be useful in the proof of Lemma F.2.

Lemma H.1. *For any $d_0 > 0$,*

$$F\left(\sqrt{\frac{nd_0}{2}}\right) \leq e^{-\beta n}, \quad \text{with} \quad \beta = \left(1 - \frac{1}{\sqrt{2}}\right)^2 d_0 - \frac{\log d_0}{2}. \quad (\text{H2})$$

Proof. Let us first compute the following n -dimensional integral (we use spherical coordinates and recall that the surface of the unit sphere in \mathbb{R}^n is $\frac{2\pi^{n/2}}{\Gamma(n/2)}$):

$$\begin{aligned} \frac{1}{\pi^{n/2}} \int_{\sum_{i=1}^n z_i^2 \geq b^2} \exp\left(-\sum_{i=1}^n z_i^2\right) dz_1 \dots dz_n &= \frac{1}{\Gamma(n/2)} \int_{R=b^2}^{\infty} R^{n/2-1} e^{-R} dR \\ &= \frac{\Gamma\left(\frac{n}{2}, b^2\right)}{\Gamma\left(\frac{n}{2}, 0\right)}. \end{aligned} \quad (\text{H3})$$

Then, translating the variable \vec{z} by \vec{a} , one obtains for $a \leq \sqrt{nd_0}$,

$$F(a) \leq \frac{1}{\pi^{n/2}} \int_{\|\vec{z}\|^2 \geq (\sqrt{nd_0}-a)^2} d\vec{z} e^{-\|\vec{z}\|^2} \quad (\text{H4})$$

$$\leq \frac{\Gamma\left(\frac{n}{2}, (\sqrt{nd_0}-a)^2\right)}{\Gamma\left(\frac{n}{2}, 0\right)}, \quad (\text{H5})$$

where the first inequality holds because the integration domain contains the one of the definition of $F(a)$, and the second is the application of Eq. H3 with $b = \sqrt{nd_0} - a$. Choosing $a = \sqrt{\frac{nd_0}{2}}$ finally gives

$$F\left(\sqrt{\frac{nd_0}{2}}\right) \leq \frac{\Gamma\left(\frac{n}{2}, nd_0 c_0\right)}{\Gamma\left(\frac{n}{2}, 0\right)}, \quad (\text{H6})$$

with

$$c_0 = \left(1 - \frac{1}{\sqrt{2}}\right)^2. \quad (\text{H7})$$

Let X be a random variable with a Poisson distribution of parameter $\lambda = nc_0d_0$ and assume n to be even, then

$$\Pr[X \leq n/2] = \frac{\Gamma(\frac{n}{2}, nd_0c_0)}{\Gamma(\frac{n}{2}, 0)}, \quad (\text{H8})$$

which implies that

$$F\left(\sqrt{\frac{nd_0}{2}}\right) \leq \Pr[X \leq n/2]. \quad (\text{H9})$$

Chernoff bound applied to a Poisson distribution of parameter λ gives:

$$\Pr[X \leq (1 - \delta)\lambda] \leq \left(\frac{e^{-\delta}}{(1 - \delta)^{1-\delta}}\right)^\lambda, \quad (\text{H10})$$

which gives here

$$F\left(\sqrt{\frac{nd_0}{2}}\right) \leq e^{-\tilde{\beta}n}, \quad (\text{H11})$$

with

$$\tilde{\beta} = c_0d_0 - \frac{1 + \log(2c_0d_0)}{2}. \quad (\text{H12})$$

Using the fact that $1 + \log(2c_0) \leq 0$, one obtains

$$F\left(\sqrt{\frac{nd_0}{2}}\right) \leq e^{-\beta n}, \quad (\text{H13})$$

with

$$\beta = c_0d_0 - \frac{\log d_0}{2}. \quad (\text{H14})$$

□

2. Proof of the lemma

One can use the same trick as in [6] and extend the Hilbert space $\bigotimes_{i=1}^n \mathcal{H}_i$ to $\bigotimes_{i=1}^n \mathcal{H}_i \otimes \mathcal{H}'_i$ and write the operator T_n as

$$T_n = \int_{\sum_{i=1}^n x_i^2 + y_i^2 \geq nd_0} \mathcal{H}' \langle 0 | U^{\otimes n} (|\vec{x}\rangle\langle\vec{x}|_{\mathbf{S}} \otimes |\vec{y}\rangle\langle\vec{y}|_{\bar{\mathbf{S}}}) U^{\dagger \otimes n} | 0 \rangle_{\mathcal{H}'} d\vec{x} d\vec{y} \quad (\text{H15})$$

where the subscripts \mathbf{S} and $\bar{\mathbf{S}}$ refer to the two possible choices of quadrature (either described by \mathbf{s} or its complement $\bar{\mathbf{s}}$), $U = e^{\pm \frac{\pi}{4}}(a \otimes a'^{\dagger} - a^{\dagger} \otimes a')$ is the beamsplitter operator and $|0\rangle_{\mathcal{H}'}$ is the vacuum state on the space $\bigotimes_{i=1}^n \mathcal{H}'_i$. The \pm sign depends on the specific choice of s . A possible choice for \mathbf{S} and $\bar{\mathbf{S}}$ would be $\mathbf{S} = \mathbf{Q} = (Q_1, \dots, Q_n)$ and $\bar{\mathbf{S}} = \mathbf{P} = (P_1, \dots, P_n)$. In this section, the bold font is used to describe vectors. We also denote $|\alpha = x + iy\rangle$ the coherent state centered in (x, y) in phase space, and will use the equality $\langle 0 | U | x \rangle_S | y \rangle_{\bar{S}} = \frac{1}{\sqrt{\pi}} |\alpha\rangle$.

Let R be the subset of \mathbb{R}^{2n} corresponding to the support of the integral above:

$$R = \left\{ (\vec{x}, \vec{y}) \in \mathbb{R}^{2n} : \sum_{i=1}^n x_i^2 + y_i^2 \geq nd_0 \right\}. \quad (\text{H16})$$

For a string $\mathbf{s} \in \{x, y\}^n$, we define the set $\mathcal{R}_{\mathbf{s}}$ as

$$\mathcal{R}_{\mathbf{s}} = \left\{ (\vec{x}, \vec{y}) \in \mathbb{R}^{2n} : \sum_{i=1}^n s_i^2 \geq n \frac{d_0}{2} \right\}. \quad (\text{H17})$$

Note in particular that the coordinates corresponding to $\bar{\mathbf{S}}$ are unbounded in this set. We also introduce the operator $\mathbf{S} = S_1 \oplus \cdots \oplus S_n$ where $S_i = Q_i(P_i)$ if $s_i = x_i(y_i)$. Noting \bar{s} the complement of s , one has for all s :

$$R \subset \mathcal{R}_{\mathbf{S}} \cup \mathcal{R}_{\bar{\mathbf{S}}} \quad (\text{H18})$$

which means that

$$T_n \leq A_{\mathbf{S}} + A_{\bar{\mathbf{S}}} \quad (\text{H19})$$

where

$$A_{\mathbf{S}} = \int_{(\vec{x}, \vec{y}) \in \mathcal{R}_{\mathbf{S}}} \mathcal{H}' \langle 0 | U^{\otimes n} (|\vec{x}\rangle\langle\vec{x}|_{\mathbf{S}} \otimes |\vec{y}\rangle\langle\vec{y}|_{\bar{\mathbf{S}}}) U^{\dagger \otimes n} | 0 \rangle_{\mathcal{H}} d\vec{x} d\vec{y}. \quad (\text{H20})$$

Here, we used the fact that the integral of $|\vec{y}\rangle\langle\vec{y}|_{\bar{\mathbf{S}}}$ on \mathbb{R}^n is equal to that of $|\vec{y}\rangle\langle\vec{y}|_{\mathbf{S}}$: this is simply the n -mode generalization of the well-known identity $\int |q\rangle\langle q| dq = \int |p\rangle\langle p| dp$ where $|q\rangle$ and $|p\rangle$ are eigenstates of the quadrature operators, Q and P , respectively. Since the previous relation holds for any string s , one has:

$$T_n \leq \frac{1}{2^n} \sum_{s \in \{x, y\}^n} A_{\mathbf{S}} + A_{\bar{\mathbf{S}}} \quad (\text{H21})$$

Let us compute the value of the operator $A_{\mathbf{S}}$:

$$A_{\mathbf{S}} = \int_{(\vec{x}, \vec{y}) \in \mathcal{R}_{\mathbf{S}}} \mathcal{H}' \langle 0 | \left(\left| \frac{\vec{x} + \vec{y}}{\sqrt{2}} \right\rangle \left\langle \frac{\vec{x} + \vec{y}}{\sqrt{2}} \right|_{\mathbf{S}} \otimes \left| \frac{\vec{x} - \vec{y}}{\sqrt{2}} \right\rangle \left\langle \frac{\vec{x} - \vec{y}}{\sqrt{2}} \right|_{\bar{\mathbf{S}}} \right) | 0 \rangle_{\mathcal{H}} d\vec{x} d\vec{y} \quad (\text{H22})$$

$$= \frac{1}{\pi^{n/2}} \int_{(\vec{x}, \vec{y}) \in \mathcal{R}_{\mathbf{S}}} e^{-\|\vec{x} - \vec{y}\|^2/2} \left| \frac{\vec{x} + \vec{y}}{\sqrt{2}} \right\rangle \left\langle \frac{\vec{x} + \vec{y}}{\sqrt{2}} \right|_{\mathbf{S}} d\vec{x} d\vec{y}. \quad (\text{H23})$$

Changing variables: $\vec{z}_1 = \sqrt{2}\vec{x}$, $\vec{z}_2 = (\vec{x} + \vec{y})/\sqrt{2}$ (that is, $\vec{x} = \vec{z}_1/\sqrt{2}$, $\vec{y} = -\vec{z}_1/\sqrt{2} + \sqrt{2}\vec{z}_2$) gives

$$A_{\mathbf{S}} = \frac{1}{\pi^{n/2}} \int_{(\vec{z}_1, \vec{z}_2) \text{ s.t. } (\vec{x}, \vec{y}) \in \mathcal{R}_{\mathbf{S}}} e^{-\|\vec{z}_1 - \vec{z}_2\|^2} |\vec{z}_2\rangle\langle\vec{z}_2|_{\mathbf{S}} d\vec{z}_1 d\vec{z}_2 \quad (\text{H24})$$

$$= \frac{1}{\pi^{n/2}} \int_{(\vec{z}_1, \vec{z}_2) \text{ s.t. } (\vec{x}, \vec{y}) \in \mathcal{R}_{\mathbf{S}}} e^{-\|\vec{z}_1 - \mathbf{S}\|^2} |\vec{z}_2\rangle\langle\vec{z}_2|_{\mathbf{S}} d\vec{z}_1 d\vec{z}_2 \quad (\text{H25})$$

$$= \frac{1}{\pi^{n/2}} \int_{\|\vec{z}_1\|^2 \geq nd_0} e^{-\|\vec{z}_1 - \mathbf{S}\|^2} d\vec{z}_1 \int_{\vec{z}_2 \in \mathbb{R}^n} |\vec{z}_2\rangle\langle\vec{z}_2|_{\mathbf{S}} d\vec{z}_2 \quad (\text{H26})$$

$$= \frac{1}{\pi^{n/2}} \int_{\|\vec{z}_1\|^2 \geq nd_0} e^{-\|\vec{z}_1 - \mathbf{S}\|^2} d\vec{z}_1 \quad (\text{H27})$$

$$= F(\mathbf{S}). \quad (\text{H28})$$

We now show for all $a > 0$, $F(\mathbf{S}) \leq P\|\mathbf{S}\|^2 \geq a^2 + F(a)\mathbb{1}$. To prove it, we need to establish that for any eigenvector $|\vec{s}\rangle$ of the operator \mathbf{S} , it holds that

$$\langle \vec{s} | F(\mathbf{S}) | \vec{s} \rangle \leq \langle \vec{s} | P\|\mathbf{S}\|^2 \geq a^2 | \vec{s} \rangle + \langle \vec{s} | F(a)\mathbb{1} | \vec{s} \rangle. \quad (\text{H29})$$

There are two possibilities,

- either $\|\vec{s}\|^2 \geq a^2$, in which case Eq. H29 reads $F(\|\vec{s}\|) \leq 1 + F(a)$, which clearly holds,
- or $\|\vec{s}\|^2 \leq a^2$, in which case Eq. H29 reads $F(\|\vec{s}\|) \leq F(a)$, which holds because $F(x)$ is an increasing function for $x \geq 0$.

Finally, one obtains

$$T_n \leq \frac{2}{2^n} \sum_{s \in \{x, y\}^n} P^{Z_n(\mathbf{s}) \geq a^2/n} + 2F(a)\mathbb{1}. \quad (\text{H30})$$

Choosing $a = \sqrt{nd_0/2}$ gives

$$T_n \leq 2W_n + 2F\left(\sqrt{\frac{nd_0}{2}}\right) \mathbb{1} \leq 2(W_n + e^{-\beta n}\mathbb{1}), \quad (\text{H31})$$

which concludes the proof of Lemma F.2.